LANDTAG
NORDRHEIN-WESTFALEN
18. WAHLPERIODE

STELLUNGNAHME
18/577

A14

FS–PP Berlin
Part mbB

Dr. iur. Rainer Frank
Rechtsanwalt · Fachanwalt für Strafrecht
Compliance Officer (Steinbeis)
Compliance Auditor (TÜV)

Dr. iur. Niklas Auffermann
Rechtsanwalt · Fachanwalt für Strafrecht
Mediator

Dr. iur. Sebastian T. Vogel
Rechtsanwalt · Fachanwalt für Strafrecht
Healthcare Compliance Officer (HCO)

Dr. iur. David Albrecht
Rechtsanwalt · Fachanwalt für Strafrecht

Dr. iur. Leonie Lo Re
Rechtsanwältin · Fachanwältin für Strafrecht
Compliance Officer (Steinbeis)
Compliance Auditor (TÜV)

Dr. iur. Michael Liedke
Rechtsanwalt

Fabian Breuer
Rechtsanwalt
Compliance Officer (Steinbeis)

Dr. iur. Viktor Volkmann, LL.M. (TCD)
Rechtsanwalt
Compliance Officer (Steinbeis)
Zert. Berater Steuerstrafrecht (FeUW)

Dr. iur. Laura Seifert
Rechtsanwältin

Sophia Hoffmeister
Rechtsanwältin

Lisa Engelbrecht
Rechtsanwältin

Potsdamer Platz 8 · 10117 Berlin

Telefon 030/31 86 85-3
Telefax 030/31 86 85-55
E-Mail mail@fs-pp.de

www.fs-pp.de

AG Chlbg. – PR 994 B

25.05.2023
63.23

An den
Rechtsausschuss
des Landtags Nordrhein-Westfalen

Löschung von Daten als Ergebnis staatsanwaltschaftlicher Ermittlungen unter Betrachtung des Urteils des Bundesverfassungsgerichts“ (Vorlage 18/1027)
Anhörung am 5. Juni 2023

Sehr geehrte Damen und Herren,

zur Vorbereitung der bezeichneten Anhörung übersende ich Ihnen nachfolgend meine schriftliche Stellungnahme zu den am 4. Mai 2023 übersandten Fragen.

Frage 1

Wie bewerten die Sachverständigen unter Berücksichtigung der Hinweise der Landesdatenschutzbeauftragten im Bericht von 2022 auf den Seiten 52-55, dass Daten von Bürgerinnen und Bürgern nicht gelöscht werden, die eigentlich zu löschen wären?

Das Recht auf informationelle Selbstbestimmung genießt Verfassungsrang. Sein wesentlicher Inhalt liegt darin, dass sein Inhaber frei über Erhebung, Speicherung, Verwendung und Weitergabe der eigenen Daten zu entscheiden. Eingriffe in die informationelle Selbstbestimmung dürfen nicht

leichtfertig erfolgen, sondern müssen sich stets am Grundsatz der Verhältnismäßigkeit messen lassen.[1] Es ist öffentlichen Stellen demnach von Verfassungs wegen grundsätzlich untersagt, personenbezogene Daten über die Grenze des Erforderlichen hinaus zu speichern oder auf andere Weise zu verarbeiten. Alleine die theoretische Möglichkeit, die Daten in Zukunft nutzen zu können, rechtfertigt eine weitere Speicherung nicht.

Für die Datenverarbeitung in polizeilichen Systemen finden diese Grundsätze ihre einfachgesetzliche Ausprägung, sofern es den Bereich der Strafverfolgung betrifft, in den §§ 483 ff. StPO und, soweit es die Gefahrenabwehr angeht, in den §§ 22 PolG NRW. Welches Regelungsregime – StPO oder PolG – zur Anwendung kommt, richtet sich nach dem Zweck der (weiteren) Datenverarbeitung: Die Verarbeitung für Zwecke eines bereits anhängigen Strafverfahrens richtet sich nach der StPO. Die Verarbeitung zum Zwecke der Gefahrenabwehr und/ oder für Zwecke künftiger Strafverfahren richtet sich nach den Polizeigesetzen (letzteres über die Verweisung in § 484 Abs. 4 StPO). Die vorliegend zu behandelnde Frage der ordnungsgemäßen Datenlöschung nach Abschluss von Strafverfahren ist somit auf Grundlage des PolG NRW zu beantworten.

§ 32 Abs. 1 PolG NRW bestimmt, dass gespeicherte personenbezogene Daten grundsätzlich zu löschen sind, soweit sie für die Erfüllung der Aufgaben der speichernden Stelle nicht mehr erforderlich sind. Zu diesem Zweck haben die verantwortlichen Stellen Termine festzulegen, zu denen *spätestens* überprüft werden muss, ob eine weitere Datenspeicherung erforderlich ist (§ 22 Abs. 2 S. 5, Abs. 4 S. 1 PolG NRW). Diese Höchstfristen entbinden die verantwortliche Stelle indes nicht von einer einzelfallbezogenen Prüfung der Rechtmäßigkeit der weiteren Datenspeicherung. Aus den vorgenannten verfassungsrechtlichen Vorgaben folgt vielmehr die Verpflichtung der verantwortlichen Stellen, durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass Datensätze mit Personenbezug *unverzüglich* gelöscht werden, sobald diese nicht mehr für die polizeiliche Aufgabenerfüllung benötigt werden.[2] Eine entsprechende Pflicht folgt auch aus Art. 16 Abs. 2 der Richtlinie (EU) 2016/680 (sog. JI-Richtlinie).

[1] BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83.
[2] *Müller/Schwabenbauer* in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, Kap. G Rn. 856.

Werden personenbezogene Daten, die für die polizeiliche Aufgabenerfüllung nicht (mehr) erforderlich sind, nicht gelöscht, ist deren weitere Speicherung somit in aller Regel rechtswidrig.[3]

Frage 2

Genügen die Erlasse des Justizministeriums vom 03.08.2022 und vom 18.01.2023, um die Löschung von nicht zu speichernden Daten sicherzustellen, so dass keine Grundrechtsverstöße eintreten?

Zunächst ist festzustellen, dass der Erlass des Justizministeriums vom 3. August 2022 insofern von einer nicht vollständig zutreffenden rechtlichen Grundlage ausgeht, als er den Eindruck vermittelt, dass § 484 StPO und § 22 PolG NRW die Speicherung eines „Basisdatensatzes“ durch die Polizeibehörden für Zwecke künftiger Strafverfahren unabhängig davon erlauben würden, ob Grund zu der Annahme besteht, dass weitere Strafverfahren gegen den Beschuldigten zu führen sind. Tatsächlich gestattet § 484 Abs. 1 StPO die Speicherung eines solchen „Basisdatensatzes“ für Zwecke künftiger Strafverfahren lediglich denjenigen Strafverfolgungsbehörden, die nicht Polizeibehörden sind. [4] Denn für letztere gilt über § 484 Abs. 4 StPO das PolG NRW, welches eine mit § 484 Abs. 1 StPO vergleichbare Befugnis nicht enthält.[5] Auch die Speicherung der in § 484 Abs. 1 StPO bezeichneten „Basisdaten“ ist der Polizei somit nur erlaubt, wenn dies im Einzelfall zur Aufgabenerfüllung, etwa für Zwecke künftiger Strafverfahren, erforderlich ist. Die Beurteilung dieser Frage setzt, worauf die LDI zu Recht hinweist, eine einzelfallbezogene Abwägung der widerstreitenden Interessen, namentlich des Interesses der betroffenen Person an einer Löschung Ihrer Daten einerseits und dem öffentlichen Interesse an einer Fortspeicherung der Daten andererseits, voraus.

Dessen ungeachtet betonen die bezeichneten Erlasse zu Recht die Notwendigkeit von zeitnahen und korrekten Mitteilung der Staatsanwaltschaften an die Polizeibehörden über die Art des Verfahrensausgangs. Die Polizeibehörden als verantwortliche

---

[3] An die Stelle der Löschung darf ausnahmsweise die Einschränkung der Verarbeitung personenbezogener Daten treten, sofern die in § 32 Abs. 3 PolG und/ oder § 50 Abs. 3 DSG NRW abschließend genannten Gründe einer Löschung im Einzelfall entgegenstehen.

[4] Ob den Strafverfolgungsbehörden die Speicherung eines „Basisdatensatzes“ für Zwecke künftiger Strafverfahren unabhängig davon erlaubt ist, ob im Einzelfall Grund zu der Annahme besteht, dass weitere Strafverfahren gegen den Beschuldigten zu führen sind, wird unter Verweis auf das verfassungsrechtliche Gebot der Erforderlichkeit zu Recht bezweifelt, vgl. OLG Hamburg StraFo 2010, 85 (87); MüKo-StPO/*Singelnstein*, § 484 Rn. 7.

[5] Vgl. SK-StPO/*Weßlau/Deiters*, 5. Aufl. 2020, § 484 Rn. 5, 22.

Stellen können die Zulässigkeit einer weiteren Datenspeicherung nur dann sachgerecht beurteilen, wenn ihnen die notwendigen Informationen über die Art sowie die Gründe für die Verfahrensbeendigung zur Verfügung stehen.

Dies kann am wirksamsten dadurch gewährleistet werden, dass bereits die Mitteilungen der Staatsanwaltschaft nach § 482 StPO i.V.m. Nr. 11 MiStra die Polizeibehörden in die Lage versetzen, die Zulässigkeit der weiteren Datenspeicherung zu beurteilen. Dies wird es mit Blick auf die Regelung des § 22 Abs. 3 S. 1 PolG NRW und dem im Übrigen bestehenden Erfordernis einer einzelfallbezogenen Interessenabwägung in aller Regel erforderlich werden lassen, dass sich die Mitteilungen näher zu den Gründen der Verfahrensbeendigung verhalten und über die in Nr. 11 MiStra bezeichneten Mindestinformationen (i.d.R. nur der Entscheidungstenor) hinausgehen. Derartige weitergehende Angaben und Erläuterungen sind nach dem Wortlaut von Nr. 11 Abs. 3 Nr. 2 MiStra nicht ausgeschlossen. Es erschließt sich vor diesem Hintergrund nicht, warum die bezeichneten Erlasse des Justizministeriums die Staatsanwaltschaften nicht dazu anhalten, ihre Mitteilungen an die Polizeibehörden bei Bedarf um die Informationen zu ergänzen, die für die Beurteilung der Zulässigkeit einer weiteren Datenspeicherung erforderlich sind. Der stattdessen im Erlass vom 18. Januar 2023 enthaltene Hinweis, dass es vor diesem Hintergrund erforderlich sein könne, dass die Polizei ihrerseits die notwendigen Informationen bei der Staatsanwaltschaft anfordert, erscheint demgegenüber weniger zielführend, weil 1. entsprechende Auskunftsersuchen der Polizei außerhalb der Weisungsbefugnis des Justizministeriums liegen und 2. der „Umweg“ über Auskunftsersuchen der Polizei weder die Verlässlichkeit des Informationsflusses erhöht, noch zur Verfahrensvereinfachung beiträgt.

Mit Blick auf die möglichen Ursachen für die von der LDI festgestellten Mängel, die (auch) in einer unzureichenden Beachtung der Mitteilungspflichten nach Nr. 11 MiStra liegen können, sind die bezeichneten Erlasse des Justizministeriums – ungeachtet der vorstehenden inhaltlichen Kritik – ein begrüßenswerter Schritt, um die Sensibilität bei den sachbearbeitenden Dezernenten insoweit zu steigern.

Frage 3

In der Entscheidung des BVerfG vom 16.2.2023 wurde auf die Problematik hingewiesen. Darin heißt es:

„Denn es können sich softwaregestützt neue Möglichkeiten einer Vervollständigung des Bildes von einer Person ergeben, wenn Daten und algorithmisch errechnete Annahmen über Beziehungen und Zusammenhänge aus dem Umfeld der Betroffenen einbezogen werden. Der Grundsatz der Zweckbindung könnte dem Eingriffsgewicht dann für sich genommen nicht hinreichend Rechnung tragen. Insgesamt ist die Methode automatisierter Datenanalyse oder -auswertung umso eingriffsintensiver, je breitere und tiefere Erkenntnisse über Personen dadurch erlangt werden können, je höher die Fehler- und Diskriminierungsanfälligkeit ist und je schwerer die softwaregestützten Verknüpfungen nachvollzogen werden können."

Wo liegen nach Ansicht der Sachverständigen die verfassungsrechtlichen Probleme in Bezug auf die Nichtlöschung von Daten, was die Landesdatenschutzbeauftragte in ihrem Bericht auf den Seiten 52 – 55 kritisiert?

Der Einsatz von automatisierten Datenanalysesystemen, wie sie Gegenstand der bezeichneten Entscheidung des BVerfG waren (und wie sie dem Grunde nach auch in § 23 Abs. 6 PolG NRW vorgesehen sind), ermöglicht es den Polizeibehörden, eine Vielzahl echter oder vermeintlicher Beziehungen zwischen Personen, Geschehnissen, Sachen und sonstigen Daten zu identifizieren, die zuvor entweder mit einem ungleich höheren menschlichen Aufwand oder gar nicht erkennbar waren. Die mit der Zusammenführung und algorithmischen Auswertung großer Datenbestände verbundenen Risiken für die Freiheitsrechte betroffener Bürgerinnen und Bürger hat das BVerfG in seiner Entscheidung anschaulich beschrieben. So besteht etwa eine gesteigerte Gefahr, dass spezielle grundrechtlich gebotene Eingriffsvorbehalte umgangen werden, indem man etwa Daten, die aus besonders eingriffsintensiven und daher nur unter spezifischen prozessualen Voraussetzungen (z.B. Richtervorbehalt) zulässigen Maßnahmen gewonnen wurden, für Zwecke verwendet werden, die eine entsprechende Datenerhebung nicht zulassen würden.[6] Außerdem befördern derartige Analysesysteme eine verfassungsrechtlich nicht unbedenkliche Vermischung von Daten aus der Gefahrenabwehr mit solchen aus der Strafverfolgung.
Das BVerfG hat darüber hinaus zu Recht auch auf die Fehler- und Diskriminierungsanfälligkeit solcher Systeme hingewiesen, die das mit der Datenverarbeitung verbunden Eingriffsgewicht erheblich steigern können. Der rechtmäßige Betrieb solcher Analysesysteme hängt somit auch maßgeblich von der Qualität der verwendeten Daten ab. Diese droht beeinträchtigt zu werden, wenn zu löschende Daten weiter ge-

[6] Vgl. dazu auch BVerfG, Beschl. v. 10.03.2008 – 1 BvR 2388/03.

speichert werden. Unterlässt es die verantwortliche Stelle etwa, die im Zusammenhang mit einem Strafverfahren erhobenen Daten eines Beschuldigten zu löschen, obwohl der Tatvorwurf inzwischen widerlegt ist, bringt der Datenbestand den Betroffenen mit einer (widerlegten) Straftat in Verbindung und kann, je nach Fallgestaltung, weitere Beziehungen zu Personen (etwa vermeintliche Zeugen) und/ oder Gegenständen (etwa vermeintliche Tatobjekte) zeigen, die nicht mit dem tatsächlichen Geschehen übereinstimmen. Der Einsatz automatisierte Analysesysteme intensiviert in solchen Fällen den mit der unzulässigen Speicherung verbundenen Eingriff in die Persönlichkeitsrechte des Betroffenen häufig noch, indem die zu Unrecht gespeicherten Daten mit weiteren Daten verknüpft werden, aus diesen Verknüpfungen unzutreffende Schlussfolgerungen gezogen werden und diese sodann die Grundlage für weitere polizeiliche Maßnahmen bilden können.
Verfassungsrechtliche Bedenken bestehen insoweit allerdings nicht nur mit Blick auf eine mangelnde Datenqualität. Bereits die (automatisierte) Weiterverarbeitung zu Unrecht gespeicherter Daten an sich stellt eine Vertiefung des in der unzulässigen Speicherung liegenden Grundrechtseingriffs dar. Der Pflicht zur ordnungsgemäßen Löschung vorhandener Daten kommt vor diesem Hintergrund eine besondere Bedeutung zu.

Frage 4

In der Entscheidung des BVerfG heißt es weiter:

> *„Dem Wortlaut nach lassen sie (Anm.: die Regelungen in den beiden Polizeigesetzen) zudem sehr weitreichende Methoden der automatisierten Datenanalyse und -auswertung zu. Der Gesetzgeber hat nicht eingegrenzt, welche Methoden der Analyse und Auswertung erlaubt sind. Die angegriffenen Vorschriften ermöglichen auch ein „Data-Mining“ bis hin zur Verwendung selbstlernender Systeme (KI). Dabei sind insbesondere auch offene Suchvorgänge zulässig. Die Datenauswertung oder -analyse darf darauf zielen, allein statistische Auffälligkeiten in den Datenmengen zu entdecken, aus denen dann, möglicherweise auch mit Hilfe weiterer automatisierter Anwendungen, weitere Schlüsse gezogen werden. Die Vorschriften schließen auch bezüglich der erzielbaren Suchergebnisse nichts aus. Nach dem Wortlaut könnte das Suchergebnis in maschinellen Sachverhaltsbewertungen bestehen – bis hin zu Gefährlichkeitsaussagen über Personen im Sinne eines „predictive policing“. Es könnten also mittels Datenanalyse oder -auswertung neue persönlichkeitsrelevante Informationen erzeugt werden, auf die ansonsten kein Zugriff bestünde. Diese potenzielle*

Weite erzielbaren neuen Wissens wird auch nicht durch eingriffsmildernde Regelungen zu dessen Verwendung flankiert.“

Wo liegen nach Ansicht der Sachverständigen die verfassungsrechtlichen Probleme in Bezug auf die Nichtlöschung von Daten, was die Landesdatenschutzbeauftragte in ihrem Bericht auf den Seiten 52 – 55 kritisiert?

Werden Daten nicht automatisiert verarbeitet, entscheidet stets ein Mensch, welche Verknüpfungen von Daten hergestellt werden sollen. Damit grenzt der Mensch auch die möglichen Verbindungen ein, die durch die Datenverarbeitung hergestellt werden können. Automatisierte Datenverarbeitungen, insbesondere solche auf der Grundlage von KI-Systemen, weisen demgegenüber ein spezifisches Risiko auf: Aufgrund der Möglichkeit, Datensätze in einem Bruchteil der Zeit analysieren zu können, wird auch eine Vielzahl von Verbindungen aufgedeckt, die ein Mensch aufgrund seiner Erfahrung von Vornherein nicht in Betracht gezogen hätte oder aufgrund Ressourcen- und Zeitmangels nicht bearbeiten konnte. Derartige Verbindungen bestehen häufig rein zufällig, also ohne kausalen Zusammenhang. Dies birgt die Gefahr, dass zuungunsten ehemals Beschuldigter in neuen Ermittlungsverfahren Zusammenhänge hergestellt werden, die keine Entsprechung in der Realität haben, aber dennoch belastende Maßnahmen nach sich ziehen können.[7] Das damit verbundene Risiko, dass Betroffene zu Unrecht polizeilicher Überwachung und/ oder sonstiger Maßnahmen ausgesetzt werden, steigt, wenn die verwendeten Analysesysteme mit veralteten, falschen oder sonst zu löschenden Daten gespeist werden.

Frage 5

Wie ist am ehesten verfassungsrechtlich sicherzustellen, dass die Staatsanwaltschaften die Vorgaben der Landesdatenschutzbeauftragten beachten und erforderliche Daten gelöscht werden?

Die verfassungsrechtlichen Vorgaben sind, wie in der Antwort auf Frage 1 skizziert, in diesem Zusammenhang klar. Es besteht allerdings augenscheinlich ein Vollzugsdefizit, das durch klare und praktisch handhabbare verwaltungsinterne Regelungen sowie eine wirksame Kontrolle verringert werden kann. Wie in der Antwort auf Frage 2 aufgezeigt, könnte eine Weisung an die Staatsanwaltschaften dergestalt, dass Mit-

[7] Müller/Schwabenbauer, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, Kap. G Rn. 1341 ff.

teilungen an die Polizei nach Verfahrensabschluss die Gründe für die Verfahrensbeendigung näher als bislang spezifizieren, Abhilfe schaffen. Ein wesentlicher Mehraufwand wäre dadurch nicht zu erwarten, da die Gründe für eine Verfahrensbeendigung, sei es im Rahmen einer Verfahrenseinstellung, eines Nichteröffnungsbeschlusses oder eines Freispruchs, ohnehin aktenkundig zu machen sind und daher eine – zumindest stichpunktartige – Mitteilung der maßgeblichen Gründe oder eine Abschrift beispielsweise der Einstellungsverfügung ohne Weiteres erfolgen könnte. Die Beachtung dieser Vorgaben wäre regelmäßig stichprobenartig zu kontrollieren.

Frage 6

Benötigen wir ein spezielles Datenverarbeitungsgesetz in NRW, aus dem sich für den Bürger auch die Rechte auf Löschung ergeben, in dem eine gesetzliche Definition des Begriffs „Restverdacht“ verankert ist, in dem Löschfristen gesetzlich verankert sind?

Derzeit enthalten sowohl das PolG NRW als auch das DSG NRW Vorschriften zur Datenverarbeitung durch die Polizeibehörden. In anderen Bundesländern existieren demgegenüber spezielle Gesetze über die Datenverarbeitung der Polizei (so etwa in Hamburg, im Saarland und in Sachsen). Wenn es auch in der Sache keinen Unterschied macht, ob datenschutzrechtliche Vorgaben in die Polizeigesetze integriert oder in einem speziellen Gesetz gebündelt sind, sprechen angesichts des mittlerweile stark angewachsenen Umfangs datenschutzrechtlicher Regelungen und deren wachsender praktischer Relevanz gute Gründe für eine gesonderte Kodifizierung in einem Datenverarbeitungsgesetz. Eine gebündelte und in sich geschlossene Regelung der Datenverarbeitung durch Polizeibehörden würde voraussichtlich auch den Rechtsanwendern die Arbeit mit diesem zunehmend komplexen Regelungsbereich erleichtern. § 50 Abs. 2 DSG NRW räumt Betroffenen bereits jetzt ein Recht auf Löschung ihrer personenbezogenen Daten ein, sofern die Verarbeitung unzulässig ist, die Daten für die Aufgabenerfüllung nicht erforderlich sind oder sonst ein Anspruch auf Löschung besteht. Insoweit besteht m.E. aktuell kein gesetzgeberischer Reformbedarf.

Eine gesetzliche Definition des Begriffs des „Restverdachts“ ist wünschenswert, zumal das PolG NRW den Begriff nicht im Zusammenhang mit einer Befugnisnorm verwendet, sondern die Zulässigkeit der Fortspeicherung wegen eines Restverdachts einer Straftat in § 22 Abs. 3 S. 2 lediglich voraussetzt. Allein aus der Verbotsnorm des § 22 Abs. 3 S. 1 PolG NRW, der zufolge eine Speicherung unzulässig ist, wenn sich

aus den Gründen der strafrechtlichen Entscheidung ergibt, dass die betroffene Person die Tat nicht oder nicht rechtswidrig begangen hat, lassen sich die an einen „Restverdacht“ zu stellenden Anforderungen nicht entnehmen. Wenn der Begriff auch mittlerweile durch die Rechtsprechung eine gewisse Konkretisierung erfahren hat, würde eine gesetzliche Begriffsbestimmung zur Rechtssicherheit beitragen. Vor allem aber sollte in diesem Regelungszusammenhang gesetzlich klargestellt werden, dass allein das Bestehen eines „Restverdachts“ noch nicht ausreicht, um eine weitere Datenspeicherung zu rechtfertigen, sondern es, worauf die LDI zu Recht hinweist, stets der Feststellung der Erforderlichkeit der Fortspeicherung im Einzelfall bedarf.

Frage 7

Ist es aus dem Grundrecht auf informationelle Selbstbestimmung geboten, dass der Beschuldigte nach Abschluss eines Strafverfahrens darüber in Kenntnis gesetzt wird, ob und in welchem Umfang seinen Daten polizeilich gespeichert bleiben oder gelöscht werden?

Eine entsprechende Informationspflicht ist m.E. nicht verfassungsrechtlich geboten. Zwar ist die polizeiliche Datenverarbeitung ein Bereich, der Bürgerinnen und Bürgern weitgehend verschlossen ist, weshalb der Gesetzgeber nach der Rechtsprechung des BVerfG hier gehalten ist, in besonderem Maße durch verfahrensbezogene Regelungen für Transparenz sorgen (vgl. BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83). Das Grundrecht auf informationelle Selbstbestimmung verpflichtet den Gesetzgeber allerdings nicht, eine spezifische Informationspflicht nach Abschluss eines Strafverfahrens zu etablieren.

Frage 8

Ist es für einen effektiven Rechtsschutz geboten, dass die öffentliche Verwaltung im Land NRW eine Zentralstelle einrichtet, die dem Beschuldigten zur Auskunft über die gespeicherten Daten/Löschung von Daten nach Abschluss eines Strafverfahrens verpflichtet ist und der gegenüber ein Löschungsanspruch besteht und auch durchgesetzt werden kann?

Eine effektive Durchsetzung von datenschutzrechtlichen Auskunftsansprüchen gegenüber der Polizei wird in der Praxis häufig durch den Umstand vereitelt, dass die Polizeibehörden über eine Vielzahl unterschiedlicher und unabhängig voneinander

geführter Datenbanken und Dateisysteme verfügen, die darüber hinaus z.T. zusammen mit Daten anderer Landes- und Bundespolizeien in Verbunddateien gespeichert werden. Eine einheitliche Überprüfung, Beauskunftung und/ oder Datenlöschung ist deshalb nur schwer ermöglicht. Häufig findet ein erfasster Vorgang Eingang in mehrere unterschiedliche Datenbanken. Zur Bearbeitung von Auskunfts- und Löschanträgen muss dann – nach meiner, auf der Außenperspektive beruhenden Kenntnis – oftmals eine große Zahl von Datenbanken einzeln abgefragt werden und im Fall von Löschungsersuchen einzeln bereinigt werden. Dies betrifft auch Daten, die im Rahmen von Strafverfahren erlangt wurden, da die verwendeten Datenbanken und Verbundsysteme eine strikte Trennung zwischen Daten, die für Zwecke der Strafverfolgung verarbeitet werden, und Daten, die für präventiv-polizeiliche Zwecke verarbeitet werden, in der Regel nicht vorsehen (sog. „Mischdateien“).[8] Zudem dürfen in Strafverfahren erhobene Daten grds. auch für Zwecke der Gefahrenabwehr verwendet werden und finden dadurch Eingang in präventiv-polizeiliche Datenbanken.

Erschwert wird die erfolgreiche Geltendmachung von Betroffenenrechten zusätzlich durch die Vielzahl von Polizeibehörden innerhalb der Bundesländer, die jeweils für die durch sie vorgenommene Datenverarbeitung verantwortlich sind, und dem Umstand, dass einzelne Behörden jeweils über eigene Datenbestände verfügen, die einem direkten Zugang durch andere Polizeibehörden entzogen sind (z.B. auf lokalen Rechnern und/ oder in behördeneigenen Datenbanken gespeicherte Daten).

Diese Situation hat zur Folge, dass Betroffene in aller Regel nicht wissen, welche Polizeibehörde Daten über sie gespeichert hat. So ist häufig bereits der richtige Adressat eines Auskunfts- und/ oder Löschungsersuchens unklar.

Vor diesem Hintergrund wäre eine zentralisierte Bearbeitung und Durchsetzung von Auskunfts- und Löschansprüchen wünschenswert, um die beschriebenen praktischen Hindernisse zu verringern. Anders als derzeit das Landesamt für Zentrale Polizeiliche Dienste sollte eine solche Zentralstelle dabei nicht lediglich als „Verteiler“ von Betroffenenanträgen an die datenschutzrechtlich verantwortlichen Polizeibehörden fungieren, sondern insoweit mit einer eigenständigen Prüf- und Anordnungskompetenz ausgestattet werden, um eine wirksame Rechtsdurchsetzung zu ermöglichen.

Insbesondere bei Daten aus Strafverfahren ist allerdings zu bedenken, dass diese oftmals länderübergreifend verarbeitet werden. Bedient sich etwa eine nordrhein-

[8] Vgl. dazu *Arzt*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Auflage 2021, Kap. G Rn. 1111 ff.

westfälische Staatsanwaltschaft im Wege der Amtshilfe polizeilichen Ermittlungspersonen in anderen Bundesländern, wie es in der Praxis häufig vorkommt, werden in aller Regel auch dort personenbezogene Daten gespeichert, die der Prüf- und Anordnungskompetenz einer Zentralstelle im Land NRW dann entzogen wären.

Die beschriebenen praktischen Probleme bei der Geltendmachung von Betroffenenrechten würden durch eine zentralisierte Bearbeitung auch aus anderen Gründen nicht vollständig behoben. Entscheidend für eine effektive Auskunftserteilung und Löschung dürfte vielmehr sein, dass durch geeignete Maßnahmen dafür Sorge getragen wird, dass auf operativer Ebene das Gebot der Datensparsamkeit beachtet wird, dass Daten richtig zugeordnet und dass Verarbeitungsvorgänge ordnungsgemäß protokolliert werden. Denn Auskunfts- und Löschungsersuchen können nur dann richtig, vollständig und in angemessener Zeit bearbeitet werden, wenn die verantwortliche Stelle die betreffenden Daten in einem möglichst standardisierten Verfahren zuverlässig identifizieren kann.

Frage 9

Wie gehen andere Bundesländer mit der Frage der Sicherstellung der Löschung von Daten durch die Justiz um?

Mir liegen keine empirischen Daten zur Löschungspraxis in der Justiz anderer Bundesländer vor. In meiner eigenen Tätigkeit als Rechtsanwalt stelle ich allerdings nicht selten fest, dass Strafverfolgungs- und Polizeibehörden verschiedener Bundesländer personenbezogene Daten aus Strafverfahren über das gesetzliche Maß hinaus speichern und erst auf Antrag des Betroffenen hin eine Löschung veranlassen. Auch dann entspricht es allerdings meiner Erfahrung, dass entsprechende Ersuchen nur mit erheblicher zeitlicher Verzögerung bearbeitet und/ oder zu Unrecht zurückgewiesen werden. Diese Wahrnehmung wird, bezogen auf das Land Berlin, gestützt durch die Feststellungen im Jahresbericht der Berliner Beauftragten für Datenschutz und Informationsfreiheit für das Jahr 2022, der zufolge „bei etwa einem Viertel der Datenauskunfts- und Löschanträge noch Bearbeitungsrückstände von sieben bis acht Monaten“ bestehen.[9]

[9] Jahresbericht der Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2022, Ziff. 2.2.

Frage 10

„Der Leitende Oberstaatsanwalt in Kleve wies darauf hin, dass die Staatsanwaltschaften gegenüber den Polizeibehörden keine Anordnungskompetenz hinsichtlich der dortigen polizeilichen Informationssysteme haben“ (Bericht des Ministeriums der Justiz vom 20.03.2023 – Vorlage 18/1027 –, Seite 6, 2. Absatz). Wie bewerten Sie diese Einschätzung?

Die Polizei unterliegt den Weisungen der Staatsanwaltschaft gem. § 161 Abs. 1 S. 2 StPO i.V.m. § 152 Abs. 1 GVG insoweit, als es um Ermittlungen in einem Strafverfahren geht. Die Weisungsbefugnis der Staatsanwaltschaft gegenüber der Polizei ist somit funktional begrenzt. Gegenstand einer staatsanwaltlichen Weisung können (nur) Ermittlungsmaßnahmen im Rahmen des Strafverfahrens sein.[10] Eine Anordnungskompetenz in Bezug auf die Löschung von in polizeilichen Informationssystemen gespeicherten Daten nach Abschluss eines Strafverfahrens hat die Staatsanwaltschaft dagegen nicht.

Dr. David Albrecht
Rechtsanwalt

[10] MüKo-StPO/*Brocke*, § 152 GVG Rn. 8.